PROBLEM SESSION

2024-02-23

16.48 PIT

$\deg f[x_1 \dots x_n] \le d$, $\boxed{H \subseteq F}$ $|H| \ge 2d$

(H^n, unif)

If $f \ne 0$ then $P_{\underline{a} \in H^n}(f(\underline{a}) = 0) \le \frac{1}{2}$

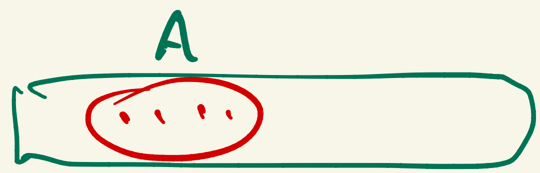
$Pr(\text{wrong answer}) \le 2^{-k}$

"If answer is "$f=0$" then $Pr(\text{wrong})$ is small"

12.69 Sorting n items

$k = o(n \log n)$ comparisons

<u>Proof</u> 2^k outcomes



$\frac{n}{100} = \ell$

$\ell!$ outcomes

$$\boxed{\frac{\ell}{n} = \varepsilon}$$

$$P(A \text{ is sorted}) \le \frac{2^k}{\ell!}$$

$$\delta < P(\exists A \text{ — " — }) \le \binom{n}{\ell} \cdot \frac{2^k}{\ell!} < \frac{n^\ell}{(\ell!)^2} \cdot 2^k$$

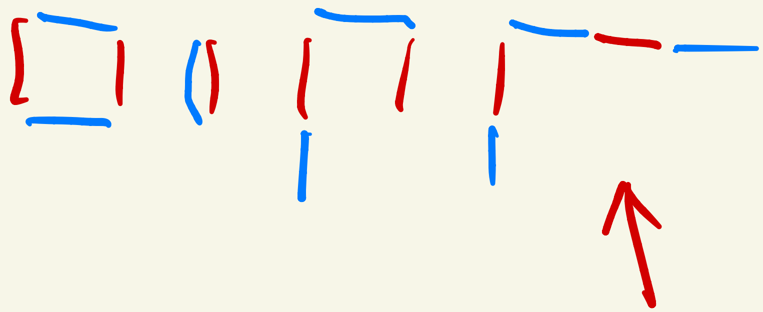
$$2^k > \delta \cdot \frac{(\ell!)^2}{n^\ell} > \delta \cdot \left(\frac{\ell^2}{e^2 n}\right)^\ell = \delta\left(\frac{\varepsilon^2}{e^2} \cdot n\right)^\ell$$

$$\ell! > \left(\frac{\ell}{e}\right)^\ell$$

$$k > \log \delta + \varepsilon n(c + \log n) \sim \varepsilon n \log n$$

13.54 M not maximum matching

$\Longrightarrow \exists$ augmenting path



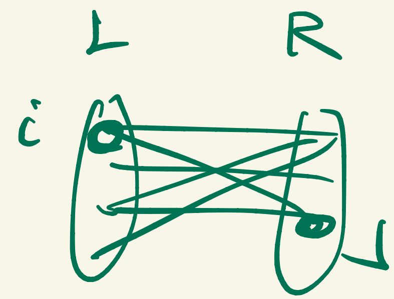
blue: maximum matching

red: non-maximum

Bipartite adj. matrix

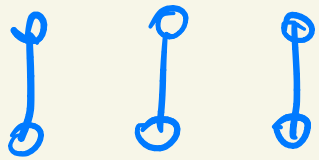
$$\begin{array}{cc} & \begin{array}{ccc} & j & R \end{array} \\ \begin{array}{c} i \to \\ L \\ \\ \end{array} & \begin{bmatrix} 0 & 1 & 1 \\ & 0 & \\ 0 & & 1 \end{bmatrix} \end{array} \qquad \begin{bmatrix} 0 & \boxed{x_1} & x_2 \\ \boxed{x_3} & 0 & \\ 0 & & \boxed{x_m} \end{bmatrix}$$

bip. adj matrix B $\qquad\qquad \hat{B}$



$\exists$ perf matching $\Longleftrightarrow$ $\det \hat{B} \neq 0$

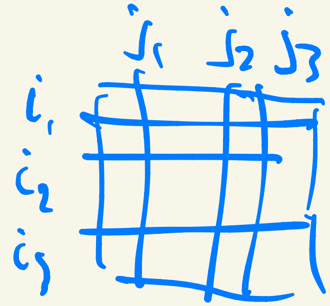
$I = \{ i_1 \quad i_2 \quad i_3 \}$



$J = \{ j_1 \quad j_2 \quad j_3 \}$

maximum matching

$\forall a \quad rk(\hat{B}(a)) \le \nu$



$\leftarrow \det \hat{B}|_{I,J} \neq 0$

$$P_{a \in H^m}\left(rk\left(\hat{B}(a)\right) = \nu \right) \ge \frac{1}{2}$$

$|H| \ge 2 \cdot \nu$

Pick p $\quad p > 2\nu \quad 4\ell > p \ge 2 \cdot \underbrace{\min(|L|, |R|)}_{\ell}$

$n^3 \log^2 n$

$\boxed{1 \mid 2 \mid 3 \mid \cancel{4} \cdot \cancel{6} \cdot \cancel{9} \mid 4\ell}$

2ℓ

Eratosthenes's sieve

$$\sum_{p \le n} \left\lfloor \frac{n}{p} \right\rfloor \sim n \sum_{p < n} \frac{1}{p} \sim n \log\log n$$

Tutte matrix

G graph

$$\begin{pmatrix} 0 & & 1 \\ & 0 & \\ 1 & \ddots & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & & x_{ij} \\ & 0 & \\ -x_{ij} & 0 & 0 \end{pmatrix}$$

adj. matrix $\rightarrow$ $C^T = -C$

skew symm matrix

$A \in F^{n \times n}$

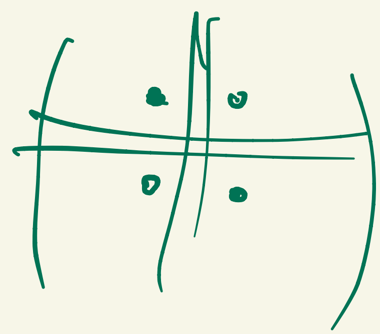
$f_A(t) = \det(tI - A)$ = charact. poly.

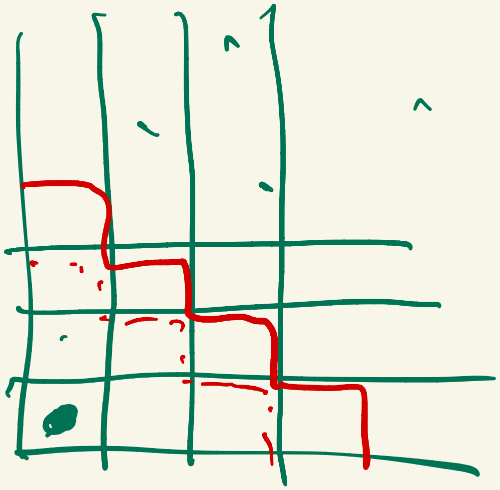
$= c_0 + c_1 t + \cdots + c_n t^n$

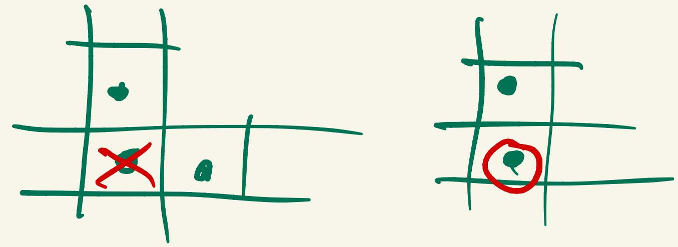
$c_n = 1$

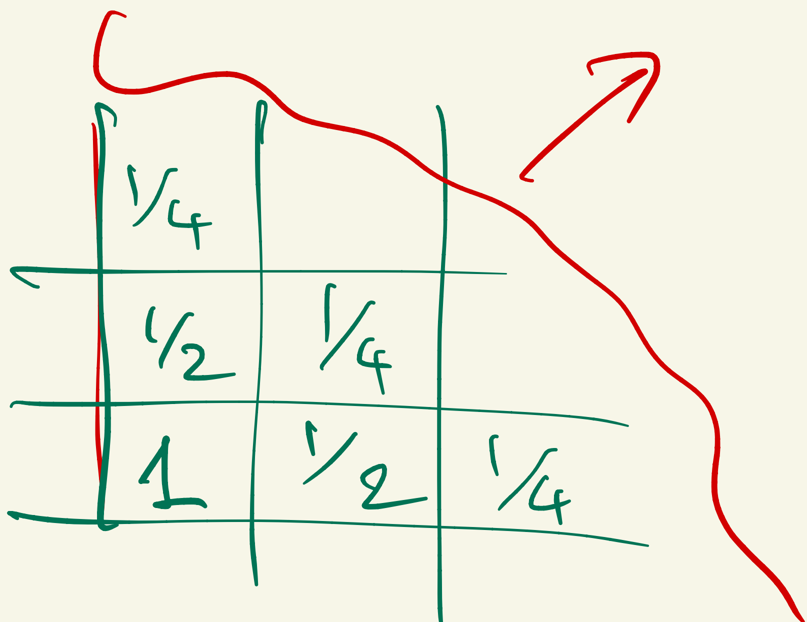
$c_{n-1} = -\sum a_{ii}$

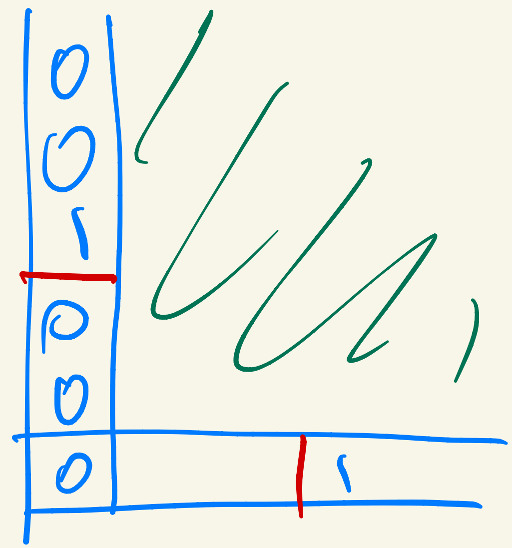
$c_{n-2} = \sum$ 2x2 symm. submatrices det











method of

<u>potential functions</u>

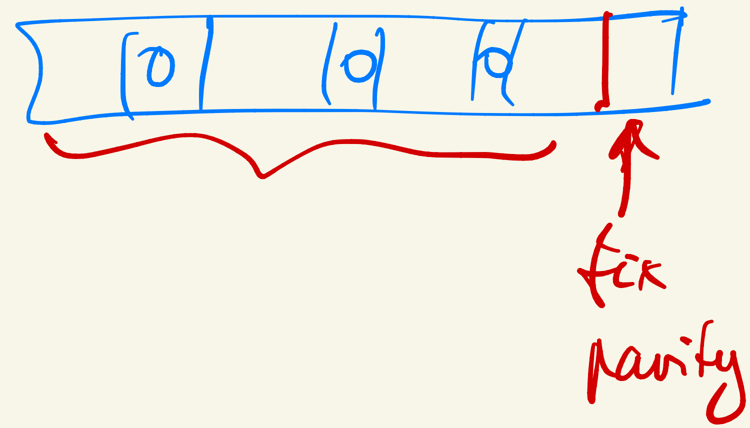
$f : \{\text{configurations}\} \to \mathbb{R}$

n events, $(n-1)$-wise but not fully indep events

$$\mathbb{F}_2^n \supset \{x \in \mathbb{F}_2^n \mid \sum x_i = 0\} =: \Omega$$

in $\mathbb{F}_2$ unif

$$A_i = \{\text{"}x_i = 0\text{"}\}$$



$$P(A_i) = \frac{1}{2}$$

$$I \subseteq [n] \qquad |I| \leq n-1$$

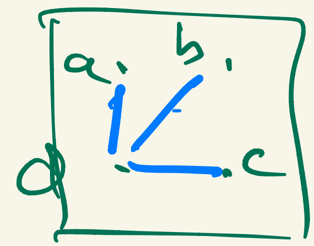
$$\Longrightarrow P\Big(\bigcap_{i \in I} A_i\Big) = \frac{1}{2^{|I|}}$$

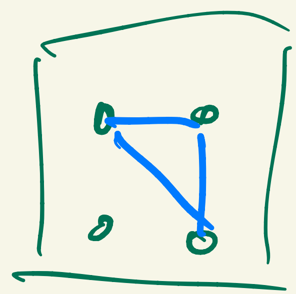
8

18-67 3 events, pairwise but not fully indep.

$|\Omega| \geq 4$

$\Omega = [4]$ unif





19.49 MAX-3SAT

disjunctive 3-clauses

$C_1, \ldots, C_m$

$\underbrace{x_i \vee \bar{x}_j \vee \bar{x}_k}_{\text{clause}}$

$\mu(C_1 \ldots C_m) =$ max # simultaneously satisfiable clauses

Claim $\mu \geq \frac{7}{8} m$

random assignment: $\Omega = \{0,1\}^n$ unf.

X = # satisfied clauses

Y_i = indicator that C_i is satisfied

$X = \sum Y_i$

$\therefore E(X) = \sum E(Y_i) = \sum P(\ \ ) = \frac{7}{8} \cdot m$

$7/8$

$A_1 \dots A_k$ indep, nontriv $\Longrightarrow |\Omega| \ge 2^k$

Pf

$A_1^{\varepsilon_1} \dots A_k^{\varepsilon_k}$ indep. $\varepsilon_i = \pm$ $A^+ = A$, $A^- = \overline{A}$

"atoms"

- $B(\varepsilon_1 \dots \varepsilon_n) = \bigcap A_i^{\varepsilon_i}$ $B(\varepsilon_1' \dots \varepsilon_n')$ $\forall\ \underline{\varepsilon} \ne \underline{\varepsilon}'$

these are disjoint

$1 = \varepsilon_i \ne \varepsilon_i' = 0$

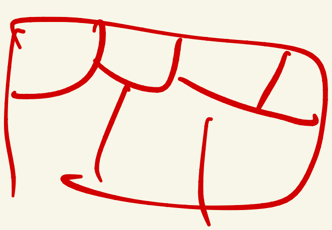
partition

$$B(\underline{\varepsilon}) \subseteq A_i$$
$$B(\underline{\varepsilon}') \subseteq \overline{A_i}$$

$$P(B(\underline{\varepsilon})) = \prod \underbrace{P(A_i^{\varepsilon_i})}_{\ne 0} \ne 0$$

2^k disjoint non-empty subsets of Ω

$\therefore |\Omega| \ge 2^k$



Ω

Fermat's Little Theorem

~~If p is prime~~

if $\gcd(a,p)=1$ then $a^{p-1} \equiv 1 \mod p$

---

for any n

$$\{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n)=1,\ a^{n-1} \equiv 1 \ (n)\}$$

nonwitnesses

$$\leq \text{subgroup of } (\mathbb{Z}/n\mathbb{Z})^\times$$

Witness for primality: for primes $\exists$ prim. root:

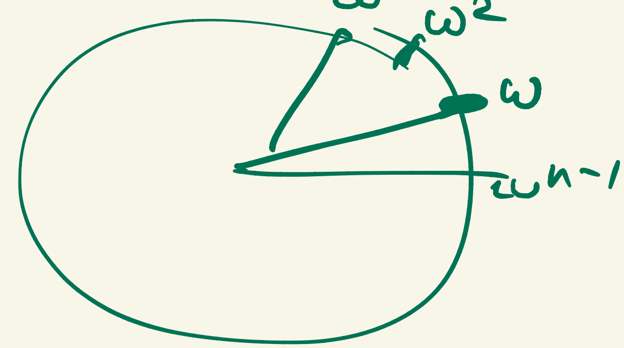
$1, g, \dots, g^{n-2} \neq 1$, $g^{n-1} = 1$ $\quad g^{\frac{n-1}{p}} \neq 1$

$$\sum n^{th} \text{ roots of unity} = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n\geq 2 \end{cases}$$

$$1, \omega, \omega^2, \dots, \omega^{n-1}$$

$$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

$$1+\omega+\dots+\omega^{n-1} = \frac{\omega^n-1}{\omega-1} = 0$$

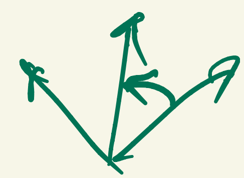


$$S = 1+\omega+\dots+\omega^{n-1}$$

$$\omega\cdot S = \omega+\omega^2+\dots+\underbrace{\omega^n}_{1} = S$$

$$(\omega-1)S = 0$$

$$S = 0$$



$\underline{S}$

$\underline{S} = \underline{S}$ rotated

$\Rightarrow \underline{S} = \underline{0}$

$$c_0 + c_1 x + \cdots + c_n x^n = \prod (x - \alpha_i) =$$

$c_n = 1$ $\qquad$ α_i : roots $\quad \alpha_i \in \mathbb{C}$

$$= x^n - \left(\sum \alpha_i\right) x^{n-1} + \sum_{i<j} \alpha_i \alpha_j \cdot x^{n-2}$$

$$x^n - 1$$